

**AMENDMENTS TO THE CLAIMS:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**LISTING OF CLAIMS:**

1. (Currently Amended) A method of securely implementing a public-key cryptography algorithm in a microprocessor-based system, the public key being composed of an integer  $n$  that is a product of two large prime numbers  $p$  and  $q$ , and of a public exponent  $e$ , said algorithm also including a private key, said method ~~consisting in~~ determining a set  $E$  comprising a predetermined number of prime numbers  $e_i$  that can correspond to the value of the public exponent  $e$ , ~~said method being characterized in that it comprises and comprising~~ the following steps ~~consisting in~~:

a) computing a value  $\epsilon = \prod_{e_i \in E} e_i$

such that  $\epsilon/e_i$  is less than  $\Phi(n)$  for any  $e_i$  belonging to  $E$ , where  $\Phi$  is the Euler totient function;

b) applying the value  $\epsilon$  to a predetermined computation involving, as a modular product, only the modular product of  $\epsilon$  multiplied by said private key of the algorithm;

c) for each  $e_i$ , testing whether the result of said predetermined computation is equal to a value  $\epsilon/e_i$ :

- if so, then attributing the value  $e_i$  to  $e$ , and storing  $e$  ~~with a view to it being used for subsequent use~~ in computations of said cryptography algorithm;

- otherwise, ~~observing~~ indicating that the computations of the cryptography algorithm using the value  $e$  cannot be performed.

2. (Currently Amended) A method according to claim 1, ~~characterized in that~~ wherein the cryptography algorithm is based on an RSA-type algorithm in standard mode.

3. (Currently Amended) A method according to claim 2, ~~characterized in that~~ wherein the predetermined computation of step b) ~~consists in~~ comprises computing a value  $C$ :

$C = \epsilon \cdot d$  modulo  $\Phi(n)$ , where  $d$  is the corresponding private key of the RSA algorithm such that  $e \cdot d = 1$  modulo  $\Phi(n)$  and  $\Phi$  is the Euler totient function.

4. (Currently Amended) A method according to claim 2, ~~characterized in that~~ wherein the predetermined computation of step b) ~~consists in~~ comprises computing a value  $C$ :

$C = e \cdot d \text{ modulo } \phi(n)$ , where  $d$  is the corresponding private key of the RSA algorithm such that  $e \cdot d = 1 \text{ modulo } \phi(n)$ , with  $\phi$  being the Carmichael function.

5. (Currently Amended) A method according to claim 1, ~~characterized in that~~ wherein the cryptography algorithm is based on an RSA-type algorithm in CRT mode.

6. (Currently Amended) A method according to claim 5, ~~characterized in that~~ wherein the predetermined computation of step b) ~~consists in~~ comprises computing a value  $C$ :

$C = e \cdot d_p \text{ modulo } (p-1)$ , where  $d_p$  is the corresponding private key of the RSA algorithm such that  $e \cdot d_p = 1 \text{ modulo } (p-1)$ .

7. (Currently Amended) A method according to claim 5, ~~characterized in that~~ wherein the predetermined computation of step b) ~~consists in~~ comprises computing a value  $C$ :

$C = e \cdot d_q \text{ modulo } (q-1)$ , where  $d_q$  is the corresponding private key of the RSA algorithm such that  $e \cdot d_q = 1 \text{ modulo } (q-1)$ .

8. (Currently Amended) A method according to claim 5, ~~characterized in that~~ wherein the predetermined computation of step b) ~~consists in~~ comprises computing two values  $C_1$  and  $C_2$  such that:

$C_1 = e \cdot d_p \text{ modulo } (p-1)$ , where  $d_p$  is the corresponding private key of the RSA algorithm such that  $e \cdot d_p = 1 \text{ modulo } (p-1)$ ;

$C_2 = e \cdot d_q \text{ modulo } (q-1)$ , where  $d_q$  is the corresponding private key of the RSA algorithm such that  $e \cdot d_q = 1 \text{ modulo } (q-1)$ ;

and ~~in that~~ wherein the test step c) ~~consists~~ comprises, for each  $e_i$ , in testing whether  $C_1$  and/or  $C_2$  is equal to the value  $e/e_i$ :

- if so, then attributing the value  $e_i$  to  $e$  and storing  $e$  ~~with a view to it being used for~~ subsequent use in computations of said cryptography algorithm;

- otherwise, ~~observing~~ indicating that the computations of said cryptography algorithm using the value  $e$  cannot be performed.

9. (Currently Amended) A method according to claim 3 ~~or claim 4~~ and in which a value  $e_i$  has been attributed to  $e$ , ~~said method being characterized in that~~ wherein the computations using the value  $e$  ~~consist in~~ comprise:

choosing a random integer  $r$ ;

computing a value  $d^*$  such that  $d^* = d + r \cdot (e \cdot d - 1)$ ; and

implementing a private operation of the algorithm in which a value  $x$  is obtained from a value  $y$  by applying the relationship  $x = y^{d^*}$  modulo  $n$ .

10. (Currently Amended) A method according to ~~any one of claims 2 to 4, and claim 2,~~ in which a value  $e_i$  has been attributed to  $e$ , ~~said method being characterized in that it consists and further including the step,~~ after a private operation of the algorithm, ~~in of~~ obtaining a value  $x$  from a value  $y$ , and ~~in that wherein~~ the computations using the value  $e$  ~~consist in~~ comprise checking whether  $x^e = y$  modulo  $n$ .

11. (Currently Amended) A method according to ~~any one of claims 5 to 8, and claim 5,~~ in which a value  $e_i$  has been attributed to  $e$ , ~~characterized in that it consists and further including the step,~~ after a private operation of the algorithm, ~~in of~~ obtaining a value  $x$  from a value  $y$ , and ~~in that wherein~~ the computations using the value  $e$  ~~consist in~~ comprise checking firstly whether  $x^e = y$  modulo  $p$  and ~~secondly~~ whether  $x^e = y$  modulo  $q$ .

12. (Currently Amended) A method according to ~~any preceding claim,~~ characterized ~~in that claim 1, wherein~~ the set  $E$  comprises at least the following  $e_i$  values: 3, 17,  $2^{16}+1$ .

13. (Currently Amended) An electronic component ~~characterized in that it comprises~~ comprising means for implementing the method according to ~~any preceding claim 1.~~

14. (Currently Amended) A smart card including ~~an~~ the electronic component ~~according to of~~ claim 13.

15. (Currently Amended) A method of securely implementing a public-key cryptography algorithm in a microprocessor-based system, the public key being composed of an integer  $n$  that is a product of two large prime numbers  $p$  and  $q$ , and of a public exponent  $e$ , said method ~~consisting in~~ determining a set  $E$  comprising a predetermined number of prime numbers  $e_i$  that can correspond to the value of the public exponent  $e$ , ~~said method being characterized in that it comprises and comprising~~ the following steps ~~consisting in:~~

- a) choosing a value  $e_i$  from the values of the set  $E$ ;
- b) if  $\delta(p) = \delta(q)$ , where  $\delta(n)$ ,  $\delta(p)$ , and  $\delta(q)$  are functions giving the number of bits encoding respectively the number  $n$ , the number  $p$ , and the number  $q$ , testing whether the chosen  $e_i$  value satisfies the relationship:

$$(1-e_i.d) \text{ modulo } n < e_i.2^{(\delta(n)/2)+1}$$

or said relationship as simplified:

$$(-e_i.d) \text{ modulo } n < e_i.2^{(\delta(n)/2)+1}$$

~~where  $\delta(p)$ ,  $\delta(q)$ , and  $\delta(n)$  are the functions giving the numbers of bits respectively encoding the number p, the number q, and the number n;~~

c) if the test relationship applied in the preceding step is satisfied ~~and so~~ defining  $e = e_i$ , and storing e with a view to using it for subsequent use in computations of said cryptography algorithm;

- otherwise, reiterating the preceding steps while choosing another value for  $e_i$  from the set E until an  $e_i$  value can be attributed to e and, if no  $e_i$  value can be attributed to e, then ~~observing~~ indicating that the computations of said cryptography algorithm using the value of e cannot be performed.

16. (Currently Amended) A method of securely implementing a public-key cryptography algorithm according to claim 15, ~~characterized in that it consists in performing wherein step b is performed~~ in the following manner when  $\delta(p)[[#]] \neq \delta(q)$ , i.e. when p and q are unbalanced, testing whether the chosen  $e_i$  value satisfies the following relationship:

$$(1-e_i.d) \text{ modulo } n < e_i.2^{g+1}$$

or said relationship as simplified:

$$(-e_i.d) \text{ modulo } n < e_i.2^{g+1}$$

with  $g = \max(\delta(p), \delta(q))$ , if  $\delta(p)$  and  $\delta(q)$  are known, or, otherwise, with  $g = \delta(n)/2 + t$ , where t designates the imbalance factor or a limit on that factor.

17. (Currently Amended) A method according to ~~claim 15 or claim 16, characterized in that~~ wherein, for all values of i,  $e_i \leq 2^{16} + 1$ , ~~and in that the step b) is replaced by another test step consisting in comprising:~~

b) if  $\delta(p) = \delta(q)$ , testing whether the chosen  $e_i$  value satisfies the relationship:

$$(1-e_i.d) \text{ modulo } n < e_i.2^{(\delta(n)/2)+17}$$

or said relationship as simplified:

$$(-e_i.d) \text{ modulo } n < e_i.2^{(\delta(n)/2)+17}$$

where  $\delta(p)$ ,  $\delta(q)$ , and  $\delta(n)$  are ~~the~~ functions giving the numbers of bits respectively encoding the number p, the number q, and the number n;

otherwise, when p and q are unbalanced, testing whether the chosen  $e_i$  value satisfies the following relationship:

$$(1-e_i.d) \text{ modulo } n < e_i.2^{g+17}$$

or said relationship as simplified:

$$(-e_i.d) \text{ modulo } n < e_i.2^{g+17}$$

with  $g = \max(\delta(p), \delta(q))$ , if  $\delta(p)$  and  $\delta(q)$  are known, or, otherwise, with  $g = \delta(n)/2 + t$ ,

where  $t$  designates the imbalance factor or a limit on that factor.

18. (Currently Amended) A method according to ~~claim 15 or claim 16, characterized in that~~ wherein step b) is replaced with another test step ~~consisting in~~ comprising:

testing whether the chosen  $e_i$  value satisfies the relationship whereby:

a predetermined number of the first most significant bits of  $(1-e_i.d)$  modulo  $n$  are zero;

or said relationship as simplified whereby:

said predetermined number of the first most significant bits of  $(-e_i.d)$  modulo  $n$  are zero.

19. (Currently Amended) A method according to claim 18, ~~characterized in that~~ wherein the test is performed on the first 128 most significant bits.

20. (Currently Amended) A method according to ~~any one of claims 15 to 19, characterized in that~~ claim 15, wherein the cryptography algorithm is based on an RSA-type algorithm in standard mode.

21. (Currently Amended) A method according to ~~any one of claims 15 to 20, and in which~~ claim 15 wherein, when an  $e_i$  value has been attributed to  $e$ , ~~said method being characterized in that~~ the computations using the value  $e$  ~~consist in~~ comprise:

- choosing a random integer  $r$ ;
- computing a value  $d^*$  such that  $d^* = d + r.(e.d - 1)$ ;

implementing a private operation of the algorithm in which a value  $x$  is obtained from a value  $y$  by applying the relationship  $x = y^{d^*}$  modulo  $n$ .

22. (Currently Amended) A method according to ~~any one of claims 15 to 20 and in which~~ claim 15 wherein, when an  $e_i$  value has been attributed to  $e$ , ~~said method being characterized in that it consists,~~ after a private operation of the algorithm, ~~in obtaining a value  $x$  is obtained~~ from a value  $y$  and ~~in that~~ the computations using the value  $e$  ~~consist in~~ comprise checking whether  $x_e = y$  modulo  $n$ .

23. (Currently Amended) A method according to ~~any one of claims 15 to 22,~~  
~~characterized in that~~ claim 15, wherein the set E comprises at least the following  $e_i$  values: 3,  
 17,  $2^{16}+1$ .

24. (Currently Amended) A method according to claim 23, ~~characterized in that~~  
~~wherein~~ the preferred choice of the values  $e_i$  from the values of the set E is made in the  
 following order:  $2^{16}+1$ , 3, 17.

25. (Currently Amended) An electronic component ~~characterized in that it comprises~~  
~~comprising~~ means for implementing the method according to ~~any one of claims 15 to 24~~  
claim 15.

26. (Currently Amended) A smart card including ~~an~~ the electronic component  
~~according to~~ of claim 25 .

27. (New) A method according to claim 15, wherein, for all values of  $i$ ,  $e_i \leq 2^{16}+1$ , step  
 b) is replaced by another test step comprising:

b) if  $\delta(p)=\delta(q)$ , testing whether the chosen  $e_i$  value satisfies the relationship:

$$(1-e_i.d) \text{ modulo } n < e_i.2^{(\delta(n)/2)+17}$$

or said relationship as simplified:

$$(-e_i.d) \text{ modulo } n < e_i.2^{(\delta(n)/2)+17}$$

where  $\delta(p)$ ,  $\delta(q)$ , and  $\delta(n)$  are functions giving the numbers of bits respectively  
 encoding the number  $p$ , the number  $q$ , and the number  $n$ ;

otherwise, when  $p$  and  $q$  are unbalanced, testing whether the chosen  $e_i$  value  
 satisfies the following relationship:

$$(1-e_i.d) \text{ modulo } n < e_i.2^{g+17}$$

or said relationship as simplified:

$$(-e_i.d) \text{ modulo } n < e_i.2^{g+17}$$

with  $g=\max(\delta(p),\delta(q))$ , if  $\delta(p)$  and  $\delta(q)$  are known, or, otherwise, with  $g=\delta(n)/2+t$ ,  
 where  $t$  designates the imbalance factor or a limit on that factor.

28. (New) A method according to claim 15, wherein step b) is replaced with another  
 test step comprising:

testing whether the chosen  $e_i$  value satisfies the relationship whereby:

a predetermined number of the first most significant bits of  $(1-e_i.d) \text{ modulo } n$  are zero;

or said relationship as simplified whereby:

said predetermined number of the first most significant bits of  $(-e_i \cdot d)$  modulo  $n$  are zero.

29. (New) A method according to claim 4 and in which a value  $e_i$  has been attributed to  $e$ , wherein the computations using the value  $e$  comprise:

choosing a random integer  $r$ ;

computing a value  $d^*$  such that  $d^* = d + r \cdot (e \cdot d - 1)$ ; and

implementing a private operation of the algorithm in which a value  $x$  is obtained from a value  $y$  by applying the relationship  $x = y^{d^*}$  modulo  $n$ .